

13 DEC 2004

PCT/JP03/07560

13.06.03

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 2 年 6 月 1 4 日

REC'D 01 AUG 2003

出 願 番 号  
Application Number: 特 願 2 0 0 2 - 1 7 4 9 9 1

[ST. 10/C]: [ J P 2 0 0 2 - 1 7 4 9 9 1 ]

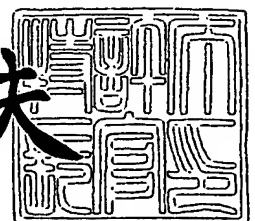
出 願 人  
Applicant(s): 株式会社ジェーシービー

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 3 年 7 月 1 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



BEST AVAILABLE COPY

出証番号 出証特 2 0 0 3 - 3 0 5 6 6 8 4

【書類名】 特許願

【整理番号】 JCB-F

【特記事項】 特許法第30条第1項の規定の適用を受けようとする特許出願

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都千代田区神田駿河台一丁目6番地 株式会社ジェーシービー 会員サービス部内

【氏名】 川本 昌由

【発明者】

【住所又は居所】 東京都千代田区神田駿河台一丁目6番地 株式会社ジェーシービー システム部内

【氏名】 入山 弘滋

【発明者】

【住所又は居所】 東京都千代田区神田駿河台一丁目6番地 株式会社ジェーシービー 情報ネットワーク部内

【氏名】 松山 永▲徳▼

【特許出願人】

【識別番号】 593022629

【氏名又は名称】 株式会社ジェーシービー

【代理人】

【識別番号】 100100402

【弁理士】

【氏名又は名称】 名越 秀夫

【選任した代理人】

【識別番号】 100088214

【弁理士】

【氏名又は名称】 生田 哲郎

## 【手数料の表示】

【予納台帳番号】 061230

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 カード発券システム及びカード発券方法

【特許請求の範囲】

【請求項 1】

顧客からの I C カード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、I C カードに書き込み、I C カードを発券する各所の拠点とにより構築されるカード発券システムに於いて、

前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信するセンター交信手段を有し、

前記拠点は、前記センター交信手段から前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記 I C カードに転送するカード交信仲介手段を有する

ことにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保することを特徴とするカード発券システム。

【請求項 2】

顧客からの I C カード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより構築されるカード発券システムに於いて、

前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点の I C カードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信するセンター交信手段を有し、

前記拠点との交信により、確実に前記カード書き込みデータを前記拠点に送信する

ことを特徴とするカード発券システム。

【請求項 3】

前記カード発券システムは、  
前記カード発行センターから前記拠点に前記カード書き込みデータを送信したと

いう交信結果を格納し、

前記カード書き込みデータを受信し I C カードに書き込まれた結果を前記拠点から受信し格納するログ管理データベースを前記カード発行センター内に有することを特徴とする請求項 1 又は請求項 2 に記載のカード発券システム。

【請求項 4】

前記カード発券システムは、  
前記拠点の端末から前記カード発行センターへのアクセスの可否を前記端末に固有の認証情報を格納している制御端末認証データベースから判断する制御端末認証手段を前記カード発行センター内に有することを特徴とする請求項 1 から請求項 3 のいずれかに記載のカード発券システム。

【請求項 5】

顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを I C カードに書き込み、前記顧客に発券する各所の拠点により構築されるカード発券システムに於いて、  
前記顧客に発券する I C カードに書き込む前記カード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記 I C カードに転送し、前記 I C カードに書き込まれた結果をネットワークを介して前記カード発行センターに送信するカード交信仲介手段を前記端末内に有し、  
前記カード発行センターとの交信により、確実に前記カード書き込みデータを前記カード発行センターから受信することを特徴とするカード発券システム。

【請求項 6】

前記カード発券システムは、  
I C カードに前記カード書き込みデータを書き込むカードリーダーライタから前記端末へのアクセスの可否を前記カードリーダーライタに固有の認証情報を格納しているリーダーライタ認証データベースから判断するリーダーライタ認証手段を前記端末内に有する

ことを特徴とする請求項 1 又は請求項 5 に記載のカード発券システム。

【請求項 7】

前記カード発券システムは、  
前記 IC カードに内蔵されたアクセス鍵と同じ鍵を用いて、  
前記 IC カードの正規、不正規を判断する  
ことを特徴とする請求項 1 から請求項 6 のいずれかに記載のカード発券システム  
。

【請求項 8】

前記カード発券システムは、  
前記拠点に於いて、顧客への新規 IC カード発行のみならず、発行済み IC カード内の個人情報やアプリケーションプログラムの書き換えを行う  
ことを特徴とする請求項 1 又は請求項 5 から請求項 7 のいずれかに記載のカード発券システム。

【請求項 9】

顧客からの IC カード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、IC カードに書き込み、IC カードを発券する各所の拠点とにより実施されるカード発券方法に於いて、  
前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信し、  
前記拠点は、前記カード発行センターから前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記 IC カードに転送する  
ことにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保することを特徴とするカード発券方法。

【請求項 10】

顧客からの IC カード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センタ

ーにより実施されるカード発券方法に於いて、  
前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点の I C カードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信し、  
前記拠点との通信により、確実に前記カード書き込みデータを前記拠点に送信すること  
ことを特徴とするカード発券方法。

【請求項 11】

前記カード発券方法は、  
前記カード発行センターから前記拠点に前記カード書き込みデータを送信したという通信結果を前記カード発行センター内のログ管理データベースに格納し、  
前記カード書き込みデータを受信し I C カードに書き込まれた結果を前記拠点から受信し前記ログ管理データベースに格納する  
ことを特徴とする請求項 9 又は請求項 10 に記載のカード発券方法。

【請求項 12】

前記カード発券方法は、  
前記拠点の端末から前記カード発行センターへのアクセスの可否を前記端末に固有の認証情報を格納している制御端末認証データベースから判断すること  
ことを特徴とする請求項 9 から請求項 11 のいずれかに記載のカード発券方法。

【請求項 13】

顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを I C カードに書き込み、前記顧客に発券する各所の拠点により実施されるカード発券方法に於いて、  
前記顧客に発券する I C カードに書き込む前記カード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記 I C カードに転送し、前記 I C カードに書き込まれた結果をネットワークを介して前記カード発行センターに送信し、  
前記カード発行センターとの通信により、確実に前記カード書き込みデータを前記カード発行センターから受信する

ことを特徴とするカード発券方法。

【請求項 14】

前記カード発券方法は、

ＩＣカードに前記カード書き込みデータを書き込むカードリーダーライタから前記端末へのアクセスの可否を前記カードリーダーライタに固有の認証情報を格納しているリーダーライタ認証データベースから判断する

ことを特徴とする請求項 9 又は請求項 13 に記載のカード発券方法。

【請求項 15】

前記カード発券方法は、

前記ＩＣカードに内蔵されたアクセス鍵と同じ鍵を用いて、

前記ＩＣカードの正規、不正規を判断する

ことを特徴とする請求項 9 から請求項 14 のいずれかに記載のカード発券方法。

【請求項 16】

前記カード発券方法は、

前記拠点に於いて、顧客への新規ＩＣカード発行のみならず、発行済みＩＣカード内の個人情報やアプリケーションプログラムの書き換えを行う

ことを特徴とする請求項 9 又は請求項 13 から請求項 15 のいずれかに記載のカード発券方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、個人情報を内蔵するＩＣカードをいかなるセキュリティ環境下にあるカード会社の拠点に於いても、セキュリティを確保し且つリアルタイムで発券するカード発券システム及びカード発券方法に関する。

【0002】

【従来の技術】

近年、ＩＣカードが普及している。ＩＣカードとは、内蔵された集積回路に、



カード番号等の固有情報や個人情報やカード用途に応じたアプリケーションプログラムを書き込んだカードであり、クレジットカードやポイントカードや交通機関の運賃カード等の複数の様々な用途に利用可能である。カードに書き込まれる情報は暗号化されている為、磁気カードやプラスチックカードに比べて偽造が困難であり、固有情報や個人情報のセキュリティが確保されるというメリットがある。

#### 【0003】

従来、カード会社等で発行される IC カードの発券処理は、IC カード自体に固有情報や個人情報等を書き込まなければならない為、高度なセキュリティ環境下に置かれたカード会社のカード発行センターに於いて行われることが主流であったが、この場合、IC カードを顧客に発行するまでに時間や輸送コストがかかり、又輸送の際のセキュリティにも気を付けなければならないという問題があった。

#### 【0004】

そこで、各所にあるカード会社の営業拠点に於いて IC カードの発券を行い、顧客のカード申込みからカード発行までの時間を短縮したシステムが、特開 2001-266076 号公開公報に開示されている。

#### 【0005】

又、従来、IC カードの発券を営業拠点に於いて行う場合は図 3 に示すように、営業拠点 2 の制御端末 21 は、カードに書き込むデータをカード発行センター 1 の書き込みデータ送信手段 17 からネットワーク 4 を介して書き込みデータ受信手段 217 に於いて受信するか、又は制御端末 21 に直接データを入力し、一旦制御端末 21 のハードディスク等の格納手段 218 にそのデータを蓄積した後に、格納手段 218 からカードリーダライタ 22 にデータを送りカード媒体 23 に書き込むという 2 段階の工程を経てカードの発券を行っていた。

#### 【0006】

##### 【発明が解決しようとする課題】

しかし、特開 2001-266076 号公開公報及び従来の発券システムに於

いてカードの発券を行う場合、営業拠点は特に路面店等の場合オープンな場所に位置することから、固有情報や個人情報等を格納している端末の盗難やこれに伴う悪用が発生する可能性があり、又営業拠点で発券処理を手掛けるオペレーターの人数も少ないので相互監視機能が十二分に働かず、営業拠点内での固有情報や個人情報の漏洩のリスクも高いので、顧客に安心して営業拠点に於ける発券システムを利用してもらうことは現状困難であると考えられる。

#### 【0007】

##### 【課題を解決するための手段】

そこで本発明者は上記問題に鑑み、従来の発券システムのような、書き込みデータを蓄積する、蓄積した書き込みデータをカードに書き込むという2段階の工程を経ることなく、いかなるセキュリティ環境下の営業拠点に於いても、顧客の安心感とセキュリティを確保し且つリアルタイムで、固有情報や個人情報等を書き込むICカードの発券を可能とするカード発券システム及びカード発券方法を発明した。

#### 【0008】

請求項1の発明は、顧客からのICカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、ICカードに書き込み、ICカードを発券する各所の拠点とにより構築されるカード発券システムに於いて、前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信するセンター交信手段を有し、前記拠点は、前記センター交信手段から前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ICカードに転送するカード交信仲介手段を有することにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保するカード発券システムである。

#### 【0009】

請求項2の発明は、

顧客からのICカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより構築されるカード発券システムに於いて、前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点のICカードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信するセンター交信手段を有し、前記拠点との交信により、確実に前記カード書き込みデータを前記拠点に送信するカード発券システムである。

【0010】

請求項5の発明は、

顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータをICカードに書き込み、前記顧客に発券する各所の拠点により構築されるカード発券システムに於いて、前記顧客に発券するICカードに書き込む前記カード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ICカードに転送し、前記ICカードに書き込まれた結果をネットワークを介して前記カード発行センターに送信するカード交信仲介手段を前記端末内に有し、前記カード発行センターとの交信により、確実に前記カード書き込みデータを前記カード発行センターから受信するカード発券システムである。

【0011】

請求項9の発明は、

顧客からのICカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、ICカードに書き込み、ICカードを発券する各所の拠点とにより実施されるカード発券方法に於いて、前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信し、前記拠点は、前記カード発行センターから前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ICカードに転送することによ

り、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保するカード発券方法である。

【0012】

請求項10の発明は、

顧客からのICカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより実施されるカード発券方法に於いて、前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点のICカードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信し、前記拠点との通信により、確実に前記カード書き込みデータを前記拠点に送信するカード発券方法である。

【0013】

請求項13の発明は、

顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータをICカードに書き込み、前記顧客に発券する各所の拠点により実施されるカード発券方法に於いて、前記顧客に発券するICカードに書き込む前記カード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ICカードに転送し、前記ICカードに書き込まれた結果をネットワークを介して前記カード発行センターに送信し、前記カード発行センターとの通信により、確実に前記カード書き込みデータを前記カード発行センターから受信するカード発券方法である。

【0014】

請求項1、2、5、9、10、13の発明により、従来の2段階のカード書き込み工程から、カード書き込みデータを端末に蓄積する工程を削除し、拠点に於いてカード番号等の固有情報や個人情報のセキュリティを確保し、且つリアルタイムでICカードの発券を行うことが出来る。

【0015】

請求項3の発明は、

前記カード発行センターから前記拠点に前記カード書き込みデータを送信したと

いう通信結果を格納し、前記カード書き込みデータを受信しＩＣカードに書き込まれた結果を前記拠点から受信し格納するログ管理データベースを前記カード発行センター内に有するカード発券システムである。

【0016】

請求項１１の発明は、

前記カード発行センターから前記拠点に前記カード書き込みデータを送信したという通信結果を前記カード発行センター内のログ管理データベースに格納し、前記カード書き込みデータを受信しＩＣカードに書き込まれた結果を前記拠点から受信し前記ログ管理データベースに格納するカード発券方法である。

【0017】

請求項３、１１の発明により、カード発行センターと拠点間の通信結果を管理し、確実にＩＣカードへのデータ書き込みを遂行することが出来る。

【0018】

請求項４の発明は、

前記拠点の端末から前記カード発行センターへのアクセスの可否を前記端末に固有の認証情報を格納している制御端末認証データベースから判断する制御端末認証手段を前記カード発行センター内に有するカード発券システムである。

【0019】

請求項１２の発明は、

前記拠点の端末から前記カード発行センターへのアクセスの可否を前記端末に固有の認証情報を格納している制御端末認証データベースから判断するカード発券方法である。

【0020】

請求項４、１２の発明により、カード発行センターへの不正アクセスを防止し、認証された拠点に於いてのみ、確実にＩＣカードの発券を遂行することが出来る。

【0021】

請求項６の発明は、

ＩＣカードに前記カード書き込みデータを書き込むカードリーダーライターから前記

端末へのアクセスの可否を前記カードリーダーライタに固有の認証情報を格納しているリーダーライタ認証データベースから判断するリーダーライタ認証手段を前記端末内に有するカード発券システムである。

【0022】

請求項14の発明は、

ICカードに前記カード書き込みデータを書き込むカードリーダーライタから前記端末へのアクセスの可否を前記カードリーダーライタに固有の認証情報を格納しているリーダーライタ認証データベースから判断するカード発券方法である。

【0023】

請求項6、14の発明により、不正なカードリーダーライタの使用を防止し、認証されたカードリーダーライタにより確実にICカードの書き込みを遂行することが出来る。

【0024】

請求項7の発明は、

前記ICカードに内蔵されたアクセス鍵と同じ鍵を用いて、前記ICカードの正規、不正規を判断するカード発券システムである。

【0025】

請求項15の発明は、

前記ICカードに内蔵されたアクセス鍵と同じ鍵を用いて、前記ICカードの正規、不正規を判断するカード発券方法である。

【0026】

請求項7、15の発明により、不正なICカードへのデータ書き込みを防止し、確実に正規のICカードへの書き込みを遂行することが出来る。

【0027】

請求項8の発明は、

前記拠点に於いて、顧客への新規ICカード発行のみならず、発行済みICカード内の個人情報やアプリケーションプログラムの書き換えを行うカード発券システムである。

【0028】

請求項 16 の発明は、  
前記拠点に於いて、顧客への新規 IC カード発行のみならず、発行済み IC カード内の個人情報やアプリケーションプログラムの書き換えを行うカード発券方法である。

【0029】

請求項 8、16 の発明により、新規の IC カード発行のみならず、IC カードの書き換え処理も、拠点に於いてセキュリティを確保し、且つリアルタイムで遂行することが出来る。

【0030】

【発明の実施の形態】

本発明の実施態様の一例を図を用いて詳細に説明する。図 1 は本発明のカード発券システムを構成するカード発行センター 1 と営業拠点 2 のシステム構成の一例である。

【0031】

カード発券システムは、高セキュリティ環境下に置かれたカード会社等のサービス提供事業体のカード発行センター 1 と、比較的低セキュリティ環境下に置かれたサービス提供事業体の営業拠点 2 との間で、専用回線 3 を介して通信を行い、主に IC カード（以下、カードと言う）の発券を営業拠点 2 で行うシステムである。尚、営業拠点 2 は全国各地に開設された顧客との窓口的役割を果たす拠点であり、サービス提供事業体の支店や子会社も含み、路面店に限らず、デパートや駅構内に設けられた店舗でもよい。

【0032】

専用回線 3 は、第三者による漏洩が不可能な電話線等の回線の中でも更に当該サービス事業体用に割り当てられた回線を使用する。これにより、カード発行センター 1 内で保有している各種情報のセキュリティ確保を行うだけでよく、各所の営業拠点 2 のセキュリティ環境の是非は問われず、営業拠点 2 等の各所でのカード発券が可能となる。以降は専用回線 3 を使用するものとして説明を行うが、専用回線 3 の代わりに第三者の漏洩が困難なネットワーク回線や、暗号化技術の

進歩に伴って第三者による各種情報の解読が不可能なネットワーク回線等を用いてもよい。又、後述の営業拠点2からカード書き込み結果を受信する為のネットワークとカード発行センター1から営業拠点2にカード書き込みデータを送信する為のネットワークは必ずしも同じ回線を使用する必要はない。

#### 【0033】

まず、カード発行センター1のシステム構成について説明する。カード発行センター1は、センター交信手段11、制御端末認証手段12、制御端末認証データベース13、書き込みデータ暗号手段14、暗号鍵データベース15、書き込み情報データベース16を有する。

#### 【0034】

センター交信手段11は、専用回線3を介して営業拠点2の制御端末21と呼ばれるコンピュータ端末と交信を行う手段である。センター交信手段11に於いては後述のように、営業拠点2の制御端末21の認証を行う為のデータ送受信を行ったり、カードに書き込むデータを暗号化したものを営業拠点2に送信したり、営業拠点2からカード書き込み結果を受信する。尚、センター交信手段11とカード交信仲介手段211との交信記録は、逐次カード発行センター1内のログ管理データベース18に格納される。

#### 【0035】

制御端末認証手段12は、営業拠点2の制御端末21の認証を行う手段である。営業拠点2の制御端末21にはそれぞれIPアドレスが割り当てられ、更に、専用回線3を介してカード発行センター1にアクセスしてきた制御端末21のみを認証許可することになっている。制御端末認証データベース13は、各制御端末21のIPアドレスを格納するデータベースである。万一、制御端末21自体が盗まれたとしても、専用回線3を介し、且つ特定のIPアドレスによってアクセスしないとカード発行センター1から不正アクセスであるとして拒否される。尚、専用回線3は複数回線用意されており、更に常時接続状態である為、複数の営業拠点2からのアクセスにも素早く対応出来る。

#### 【0036】

書き込みデータ暗号手段14は、カードの入会申込みや入会申込み内容に基づ



いた審査が完了し、カード発券待ち状態となっているユーザのカードに書き込むべき個人情報やカード番号等の固有情報やアプリケーションプログラム等の書き込みデータを書き込み情報データベース16に格納しておき、営業拠点2からカード発券要求があった場合に書き込みデータを暗号鍵データベース15に格納されている暗号鍵によって暗号化する手段である。尚、個人情報には、氏名等の基本情報の他にアプリケーションプログラム（例えばクレジット用アプリケーションや、ポイントシステム用アプリケーション）毎に必要なクレジット支払い設定や与信枠やポイント数等が含まれる。又、アプリケーションプログラムは工場出荷時に既にカードに書き込まれている場合もある。

#### 【0037】

次に、営業拠点2のシステム構成について説明する。営業拠点2は、制御端末21、カードリーダーライタ22を有する。

#### 【0038】

制御端末21は、更にカード交信仲介手段211、入出力端末214、暗号復号手段212、鍵情報データベース213、リーダーライタ認証手段215、リーダーライタ認証データベース216を有するコンピュータ端末である。制御端末21は従来の制御端末21（図3参照）と比較して、格納手段218を有さないことが本発明の大きな特徴である。

#### 【0039】

カード交信仲介手段211は、専用回線3を介して制御端末21毎に固有のIPアドレスでカード発行センター1にアクセスする手段であり、又、カード発行センター1からカードへの書き込みデータを受信し、後述のカードリーダーライタ22に転送してカード発行センター1とカード間の仲介を行ったり、入出力端末214の内、キーボード等の入力端末を用いてカード発行センター1へのアクセス要求や特定顧客のカード発券依頼を行ったり、ディスプレイやプリンタ等の出力端末を用いて発券結果出力やカード発行センター1からの指示受信の表示を行う。

#### 【0040】

暗号復号手段212は、カード発行センター1から受信した暗号化済みの書き

込みデータを鍵情報データベース213内に格納されている復号鍵（カード発行センター1内の暗号鍵データベース15に格納されている暗号鍵と対の関係にある）によって復号し、カードリーダーライタ22に挿入された工場出荷状態のカードに予め内蔵されているアクセス鍵と同様の、鍵情報データベース213に格納されているアクセス鍵を用いてカードへのアクセスを可能とした後、一度復号された書き込みデータをカード書き込み用の暗号鍵によって暗号化する方法である。尚、鍵情報データベース213及び暗号復号手段212はブラックボックス化されており、万一制御端末21を盗まれたとしても、鍵情報データベース213から鍵情報自体を読みとることは困難な仕組みとなっており、制御端末21には個人情報データを蓄積しないので個人情報の流出も不可能である。更には、後述のカードリーダーライタ22に不正なカードを挿入し、書き込みデータを書き込もうとした場合、鍵情報データベース213に格納されているアクセス鍵と同じ鍵を内蔵したカードでないとカードへの書き込みは行えない為、不正なカードからのアクセスはこの時点で拒否され、鍵情報だけがあっても意味がないということになる。又、この暗号復号手段212と鍵情報データベース213による暗号化と復号化の処理工程は、営業拠点2の制御端末21が有している必要は必ずしもなく、カード発行センター1内の書き込みデータ暗号手段14に於いて最初からカード書き込み用の暗号鍵によって暗号化した書き込みデータを制御端末21のカード交信仲介手段211に送信し、カード発行センター1内の暗号鍵データベース15に保有しているアクセス鍵を用いて、カード発行センター1からカードにアクセスすることによって、直接カードへの書き込みを行ってもよい。この場合も、制御端末21のカード交信仲介手段211は単に、カード発行センター1とカード間の仲介を行うに過ぎないものである。

#### 【0041】

リーダーライタ認証手段215は、後述のカードリーダーライタ22を制御端末21に接続する際に、カードリーダーライタ22の認証を行う手段である。即ち、不正なカードリーダーライタ22はカードの書き込み及び読み取りに使用出来ない。リーダーライタ認証データベース216に格納されているカードリーダーライタ22固有の認証情報を元に認証を行い、不正なカードリーダーライタ22とのアクセス

は拒否する。

#### 【0042】

カードリーダーライタ 22 は、工場出荷状態のカード媒体 23 を挿入し、前述のように暗号復号手段 212 によってカードへのアクセスを可能とした後、カード交信仲介手段 211 を介してカード発行センター 1 から受信した書き込みデータをカード媒体 23 に直接転送してリアルタイムに書き込む手段であり、予め制御端末 21 のリーダーライタ認証手段 215 に於いて認証されたカードリーダーライタ 22 のみが使用可能である。更にカード媒体 23 に書き込みデータが書き込まれたかどうかを、カード媒体 23 からカードリーダーライタ 22 に於いて読みとり、カード交信仲介手段 211 を介してセンター交信手段 11 に伝達することにより、あたかもカード発行センター 1 とカードが直接交信しているのと同じ状態になり、仮に不正なデータが書き込まれたとしてもカード発行センター 1 で交信結果を随時受信することにより、不正かどうかをチェックすることが出来る。又、個人情報を含む書き込みデータが営業拠点 2 に蓄積されることはないので、従来のような蓄積、書き込みという 2 段階の工程を経る必要がなくなり、セキュリティを確保し、且つリアルタイムで営業拠点 2 に於けるカードの発券が可能となる。尚、カードにデータを書き込んだり、カード内のデータを読みとることが出来る手段があれば、カードリーダーライタ 22 には限定されない。

#### 【0043】

##### 【実施例】

次に本発明のプロセスの流れの一例を図 2 のフローチャート図及び、図 1 のシステム構成図とを用いて詳細に説明する。尚、本実施例については、顧客が営業拠点 2 に出向き、カードの発券を要求した場合について説明するが、顧客は既に営業拠点 2 又はカード発行センター 1 でカード発行の為の入会申込みを F A X や電話や電子メールにより行い、カード発行センター 1 に於ける審査を経て、顧客に発行するカードに書き込む為の書き込みデータをカード発行センター 1 内の書き込み情報データベース 16 内に格納しているものとする。

#### 【0044】

営業拠点 2 の制御端末 2 1 は、カード交信仲介手段 2 1 1 により、専用回線 3 を介してカード発行センター 1 のセンター交信手段 1 1 にアクセスを要求する (S 2 1 0)。

#### 【0045】

センター交信手段 1 1 は制御端末 2 1 からのアクセス要求を受信し、制御端末認証手段 1 2 に於いて、制御端末 2 1 に固有の IP アドレスとアクセスしてきた専用回線番号により、制御端末認証データベース 1 3 内に合致する IP アドレスがあるかを確認し、制御端末 2 1 のアクセスを許可する (S 2 2 0)。IP アドレスが異なる、専用回線 3 を介していない等の不正なアクセスの場合にはアクセスを不許可とし、カード発券が行えないことを通知する (S 3 1 0)。

#### 【0046】

アクセスを許可された制御端末 2 1 は、センター交信手段 1 1 に顧客の書き込みデータを要求する旨をカード交信仲介手段 2 1 1 から送信する (S 2 3 0)。例えば、入出力端末 2 1 4 からカード発券対象となる顧客の ID やパスワードを入力して送信する。

#### 【0047】

センター交信手段 1 1 は、カード交信仲介手段 2 1 1 に対して、営業拠点 2 のカードリーダーライタ 2 2 を制御端末 2 1 と接続し、カードリーダーライタ 2 2 にカードを挿入するよう要求する (S 2 4 0)。尚、センター交信手段 1 1 とカード交信仲介手段 2 1 1 のやりとりは都度、リアルタイムで入出力端末 2 1 4 にも表示される。

#### 【0048】

カード交信仲介手段 2 1 1 はカード挿入要求を受信し、制御端末 2 1 にカードリーダーライタ 2 2 を接続し、更にカードを挿入する (S 2 5 0)。尚、カードリーダーライタ 2 2 は制御端末 2 1 のリーダーライタ認証手段 2 1 5 により、接続許可を受けている正規のカードリーダーライタ 2 2 であるものとする。

#### 【0049】

挿入されたカードとカード発行センター 1 との間で交信が開始される (S 2 6 0)。まず、制御端末 2 1 内の暗号復号手段 2 1 2 によって、カードに内蔵され

ているアクセス鍵と同様の鍵情報データベース 213 内のアクセス鍵により、カードにアクセスする。不正なカードかどうかは、アクセス鍵自体が存在しなかったり、鍵情報データベース 213 内に格納されているアクセス鍵と異なる鍵がカードに内蔵されていること等から判別することが出来る。不正なカードや、カード内のチップが壊れている等の不良カードである場合は、正規のカードをカードリーダーライター 22 に挿入し、再試行する (S255)。

#### 【0050】

カード交信仲介手段 211 から受信したセンター交信手段 11 は、書き込みデータ暗号手段 14 により書き込み情報データベース 16 に格納された該当顧客の書き込みデータを暗号化し送信する (S270)。

#### 【0051】

カード交信仲介手段 211 は、暗号化された書き込みデータを受信し、暗号復号手段 212 に於いてカード発行センター 1 で暗号化した暗号鍵と対になっている鍵情報データベース 213 内の復号鍵によって書き込みデータを復号し、更にカードに書き込む為の暗号鍵でその書き込みデータを暗号化した後に、カードリーダーライター 22 に転送し、挿入されているカードに書き込みを行う (S280)。この時、制御端末 21 及びカードリーダーライター 22 には書き込みデータの蓄積は行わず、リアルタイムで暗号、復号処理及びカードへの書き込みを行う。

#### 【0052】

カードリーダーライター 22 への転送結果、カードへの書き込み可否をカード交信仲介手段 211 からセンター交信手段 11 に送信する (S290)。書き込みが行えなかった場合はその旨をセンター交信手段 11 に於いて受信し、センター交信手段 11 から書き込みデータを再送する等の処置をとる。尚、センター交信手段 11 とカード交信仲介手段 211 との双方の交信結果の履歴は、カード発行センター 1 側のログ管理データベース 18 に逐次格納しておくことが望ましい。万一、交信途中で電源が遮断された、アクセス不可能になった等のトラブルが発生した時でも、元の状態に回復させることが可能となる。又、カードに不正なデータが書き込まれた場合は、ログ管理データベース 18 内の交信結果からカード発行センター 1 に於いて判別することが出来る。

## 【0053】

書き込み情報データベース16に、まだ書き込みデータが残っている場合は、前の書き込みデータが確実にカードに書き込まれたという結果をカード交信仲介手段211から受信したことを先に確認してから、センター交信手段11から次の書き込みデータをカード交信仲介手段211に送信する(S300)。尚、最後の書き込みデータであれば、最後であることが分かるフラグ等を付して書き込みデータとともに送信する。

## 【0054】

カード交信仲介手段211に於いて受信した書き込みデータは、先のS280、S290と同様のステップでカードへの書き込みを行う。又、最後の書き込みデータを受信した時は、再度アクセス鍵を用いてアクセスを終了する等して、カードへの書き込みを閉じる処理をカードリーダーライタ22側で行い、カード書き込みが正常に終了したことをカード交信仲介手段211からセンター交信手段11に送信する。

## 【0055】

別の顧客のカード発券を行う場合は、S230に戻り、同様の手順でカード発行センター1間と制御端末21間で交信を行う(S320)。

## 【0056】

以上のように、営業拠点2の制御端末21内には書き込みデータを蓄積せず、あくまで制御端末21は直接カード発行センター1とカード間の仲介の役割を果たすことにより、固有情報や個人情報のセキュリティを確保し且つリアルタイムでカードの発券を行うことが出来る。

## 【0057】

本発明に於ける各手段、データベースは、その機能が論理的に区別されているのみであって、物理上あるいは事実上は同一の領域を為していてもよい。又データベースの代わりにデータファイルであってもよいことは言うまでもなく、データベースとの記載にはデータファイルをも含んでいる。

**【0058】****【発明の効果】**

本発明により、いかなるセキュリティ環境下に置かれた各所の営業拠点に於いても、顧客が安心してカード発券を要求することが可能となり、更なるＩＣカードの普及につながる。

**【0059】**

顧客の要求に応じて、リアルタイムでＩＣカードを発券することが可能となるので、カード会社の営業拠点のみならず、空港や鉄道の駅やデパートの窓口等でもＩＣカードの発券を行うことが出来る。急ぎの顧客にも便利である。

**【0060】**

ＩＣカードに書き込む情報は営業拠点内に蓄積されないので、営業拠点の店員を始め、周囲にいる者や第三者に知られることが絶対になく、カード会社以外の業者がカード発券を代行することも出来る。

**【0061】**

新規発券に限らず、既に発行されているＩＣカードに書き込まれている個人情報やアプリケーションプログラムの書き換え、変更を行う際にも本発明は有用であり、カード発行センターに書き込み用データさえ格納されていれば、営業拠点でのカード書き換えが可能となり、わざわざカード発行センターで書き換える必要がないので、時間と輸送コストの削減につながる。

**【図面の簡単な説明】**

【図１】 本発明のカード発券システムのシステム構成の一例を示す図である。

【図２】 本発明のプロセスの流れの一例を示すフローチャート図である。

【図３】 従来の営業拠点に於けるカード発券システムの構成の一例を示す図である。

**【符号の説明】**

１：カード発行センター

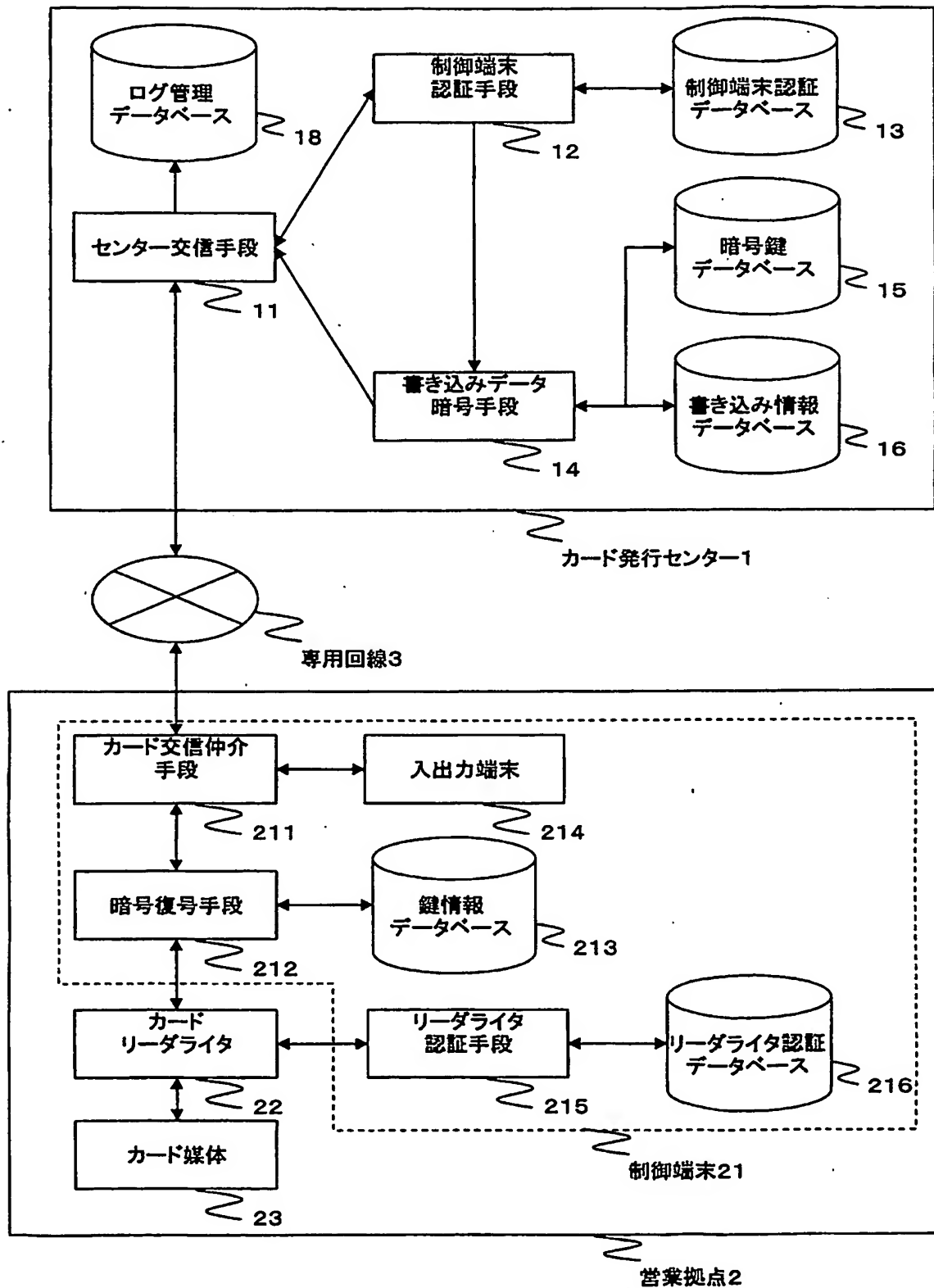
１１：センター交信手段

- 12 : 制御端末認証手段
- 13 : 制御端末認証データベース
- 14 : 書き込みデータ暗号手段
- 15 : 暗号鍵データベース
- 16 : 書き込み情報データベース
- 17 : 書き込みデータ送信手段
- 18 : ログ管理データベース
- 2 : 営業拠点
- 21 : 制御端末
- 211 : カード交信仲介手段
- 212 : 暗号復号手段
- 213 : 鍵情報データベース
- 214 : 入出力端末
- 215 : リーダライタ認証手段
- 216 : リーダライタ認証データベース
- 217 : 書き込みデータ受信手段
- 218 : 格納手段
- 22 : カードリーダーライタ
- 23 : カード媒体
- 3 : 専用回線
- 4 : ネットワーク

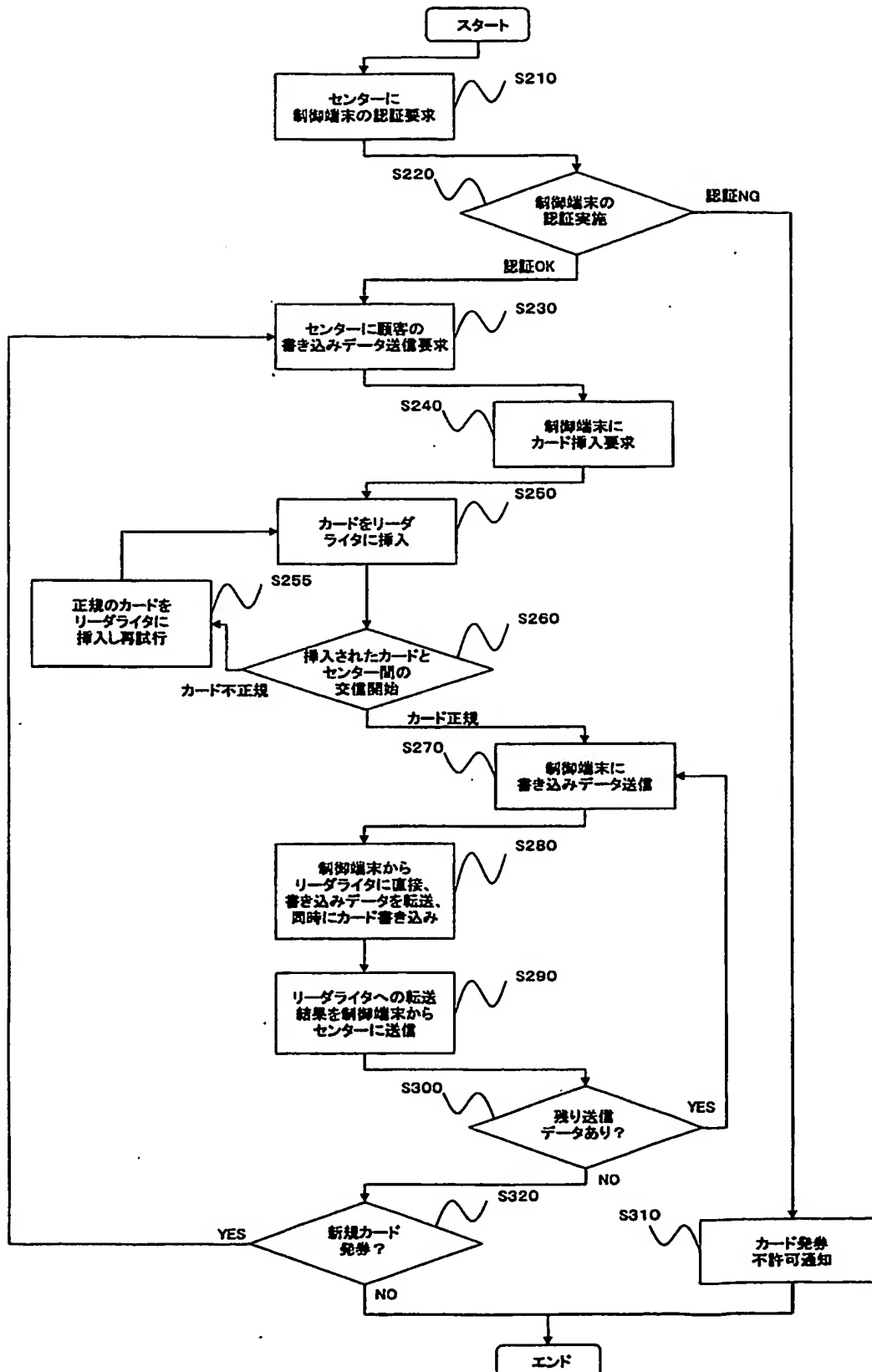


【書類名】 図面

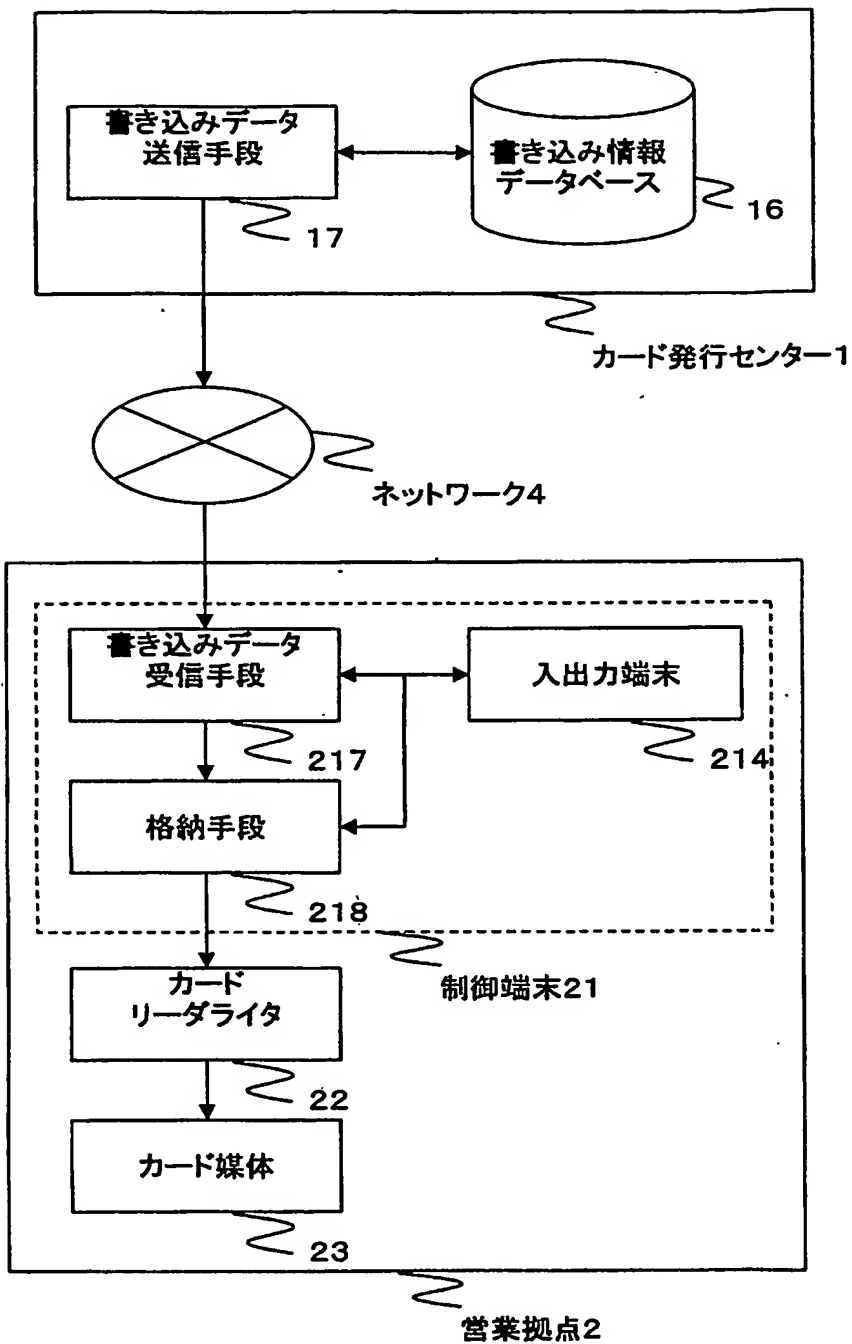
【図1】



【図 2】



【図 3】



【書類名】 要約書

【要約】

【課題】

顧客の個人情報の内蔵する IC カードをいかなるセキュリティ環境下にあるカード会社の拠点に於いても、セキュリティを確保し且つリアルタイムで発券する。

【解決手段】

カード発行センターは、顧客のカード書き込みデータを拠点に送信するセンター交信手段を有し、前記拠点は、前記センター交信手段から前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された IC カードに直接転送するカード交信仲介手段を有するカード発券システムである。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2002-174991
受付番号	50200871727
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年 7月26日

<認定情報・付加情報>

【提出日】	平成14年 6月14日
-------	-------------

次頁無

特願 2002-174991

出 願 人 履 歴 情 報

識別番号

[593022629]

1. 変更年月日

1993年 2月 2日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台1丁目6番地

氏 名

株式会社ジェーシービー

2. 変更年月日

2003年 5月29日

[変更理由]

住所変更

住 所

東京都港区南青山五丁目1番22号

氏 名

株式会社ジェーシービー